SOPHOS

The State of Ransomware 2025

Jon Hope
Senior Technology Evangelist
Jon@Sophos.com

SOPHOS

About Me.....

Technology Evangelist, Ex-Channel Manager
Senior Channel Sales Engineer
Joined Sophos in 2011
Marketing Director of a Pet Care Business
Keen Sailor, Passion for Photography
Father of two wonderful boys

Jon Hope

Jon@sophos.com

Observing the Landscape

Sophos Counter Threat Unit

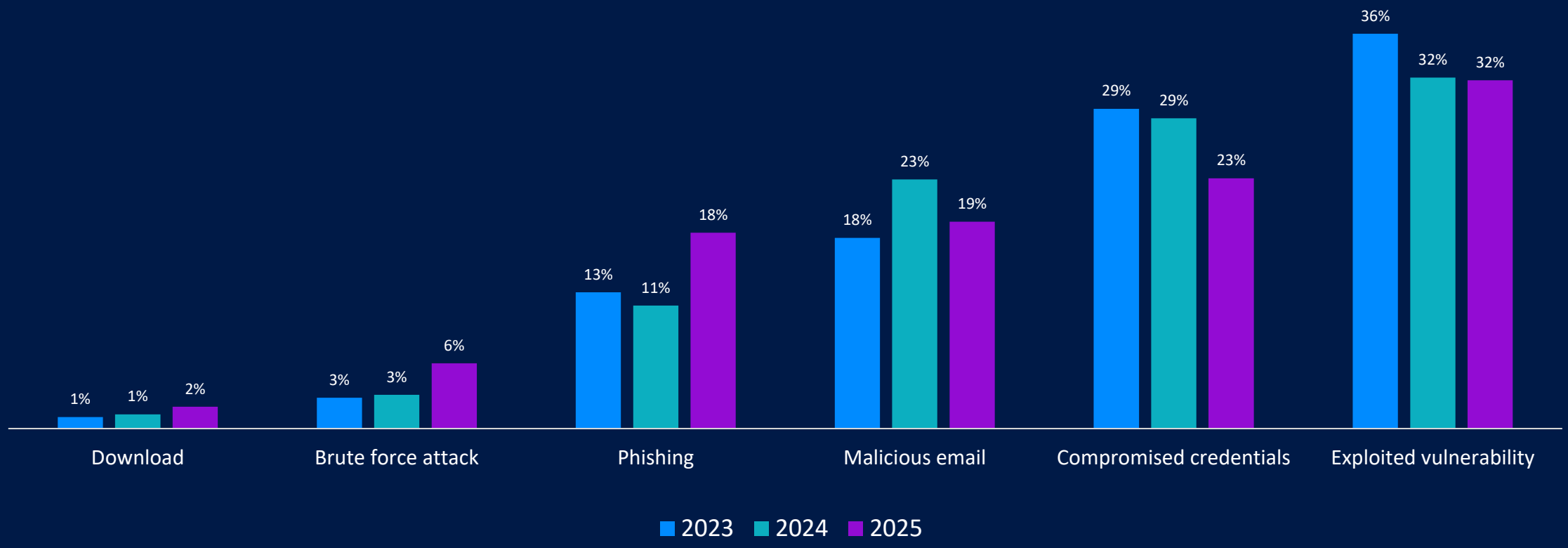
Findings from an Independent, Vendor-Agnostic Survey

SOPHOS

Why Organizations Fall Victim

Technical Root Cause of Attacks

For the third year running, exploited vulnerabilities are the top-reported root cause of ransomware attacks



Do you know the root cause of the ransomware attack your organization experienced in the last year? Yes. n=3,400 (2025), 2,974 (2024), 1974 (2023).

SOPHOS

Identity is the Fuel of the Cybercriminal Ecosystem

IAM MISCONFIGURATIONS

95% of organizations have a critical Microsoft Entra ID identity misconfiguration.

Source: incident response engagements conducted by Sophos

IDENTITY -BASED ATTACKS

90% of organizations experienced an identity breach in the past year.

Source: IDSA Trends in Securing Digital Identities, 2024

LEAKED AND STOLEN CREDS

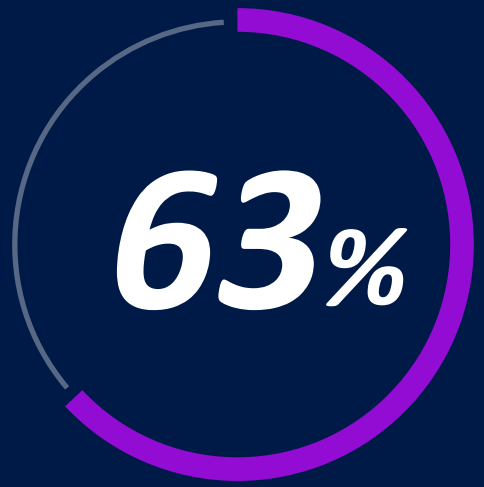
The number of stolen credentials for sale on the dark web has more than doubled in the past year.

Source: Sophos X-Ops Counter Threat Unit (CTU) data, June 2024 – June 2025

Organizational Root Cause of Attacks

Organizational Root Cause of Attacks

Victims are typically facing multiple organizational challenges with respondents citing 2.7 factors, on average, that contributed to them falling victim to the ransomware attack.



PROTECTION CHALLENGES

Lack of protection or poor-quality protection solutions that could not stop the attack

RESOURCE CHALLENGES

Lack of human expertise (skills or capacity) to detect and stop the attack in time

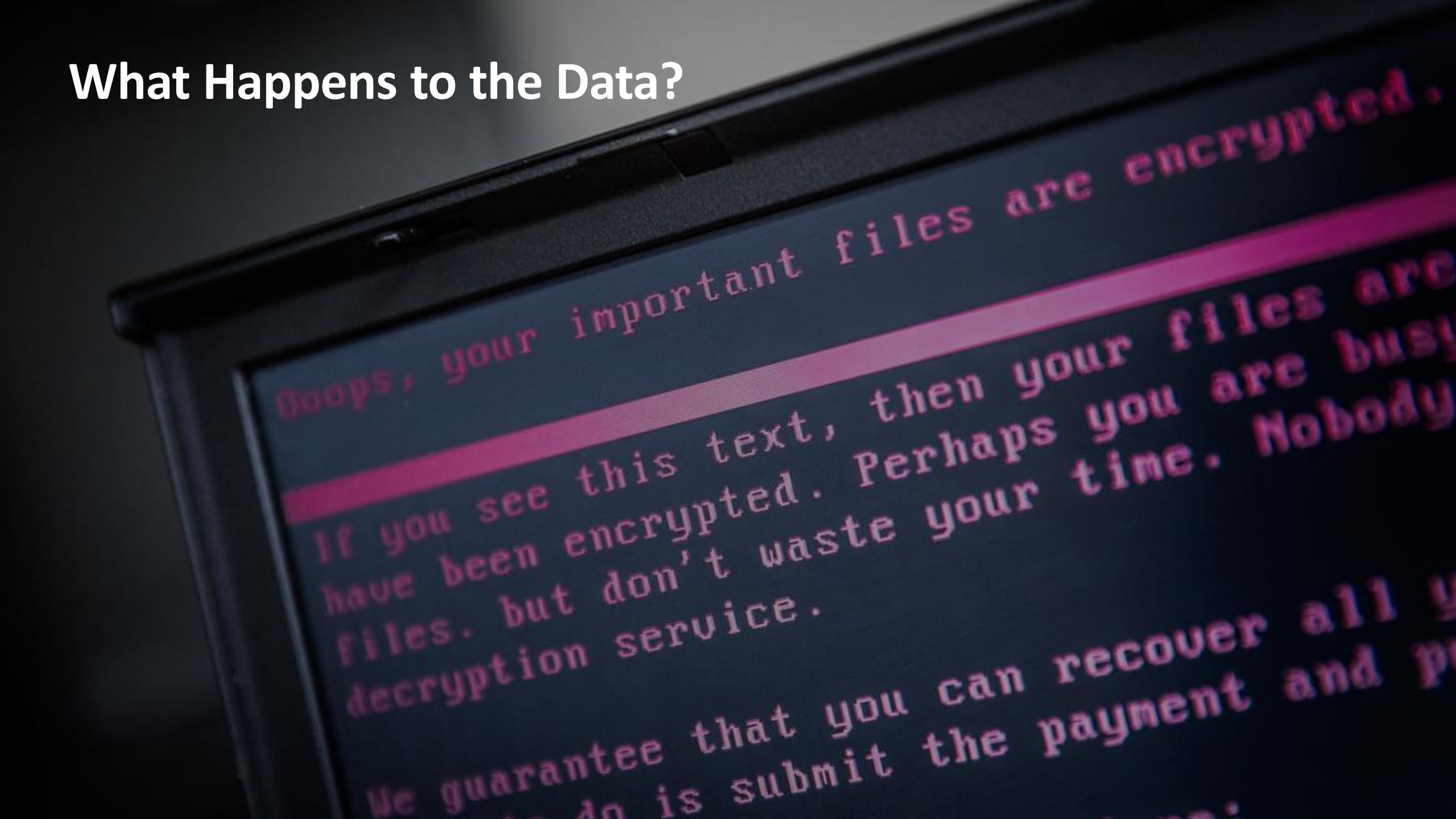
SECURITY GAP

Had a known or unknown weakness in their defenses Known or unknown

Why do you think your organization fell victim to the ransomware attack? n=3,400. Consolidated responses.

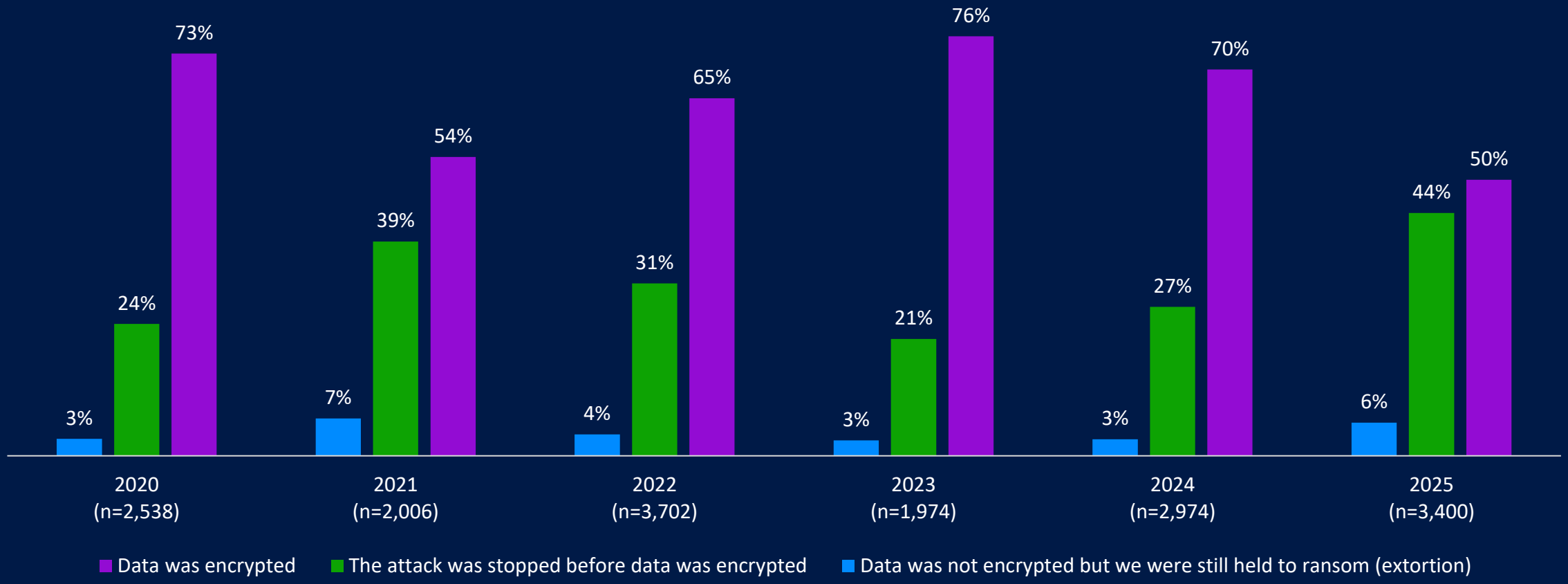
SOPHOS

What Happens to the Data?



Data Encryption Rate

Data encryption is at the lowest rate in six years. At the same time, the percentage of organizations whose data was not encrypted but they were held to ransom anyway (extortion) doubled in the last year.



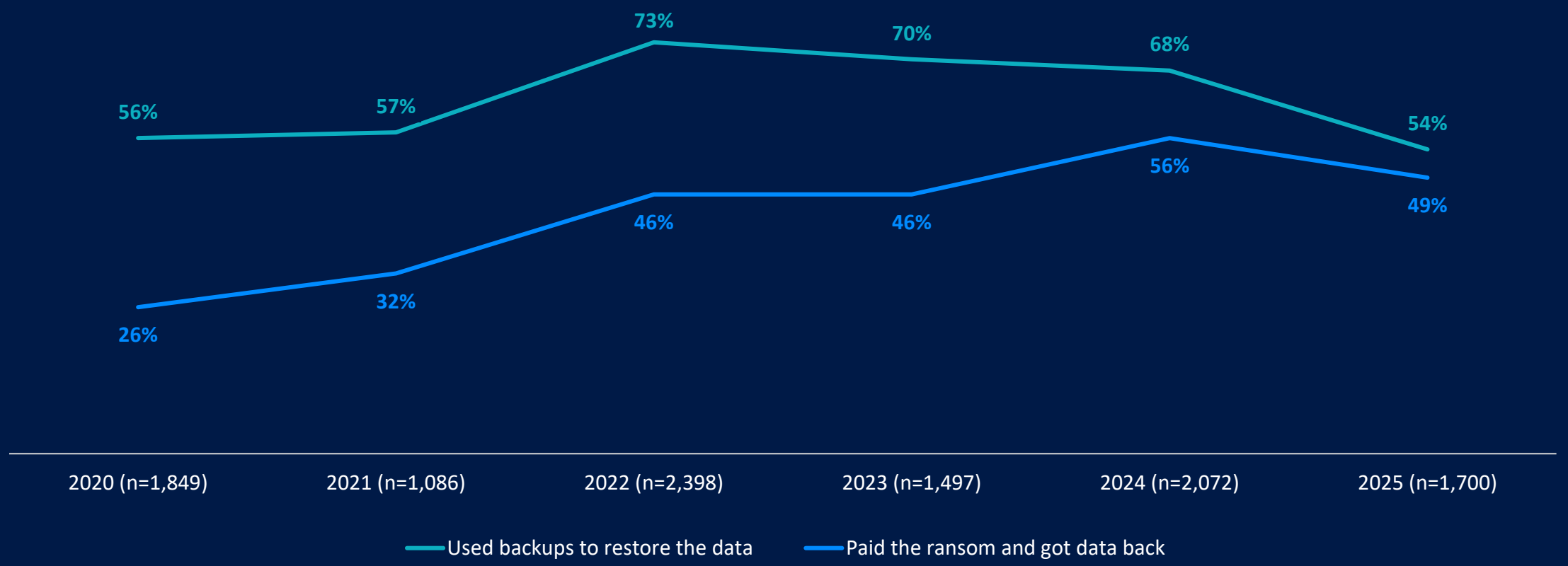
Did the cybercriminals succeed in encrypting your organization's data in the ransomware attack? Base numbers in chart.

SOPHOS

Ransom and Recovery

Recovery of Encrypted Data

The percentage of ransomware victims that recovered encrypted data through backups has fallen for the third year in a row. Data recovery through backups is at its lowest rate in six years.



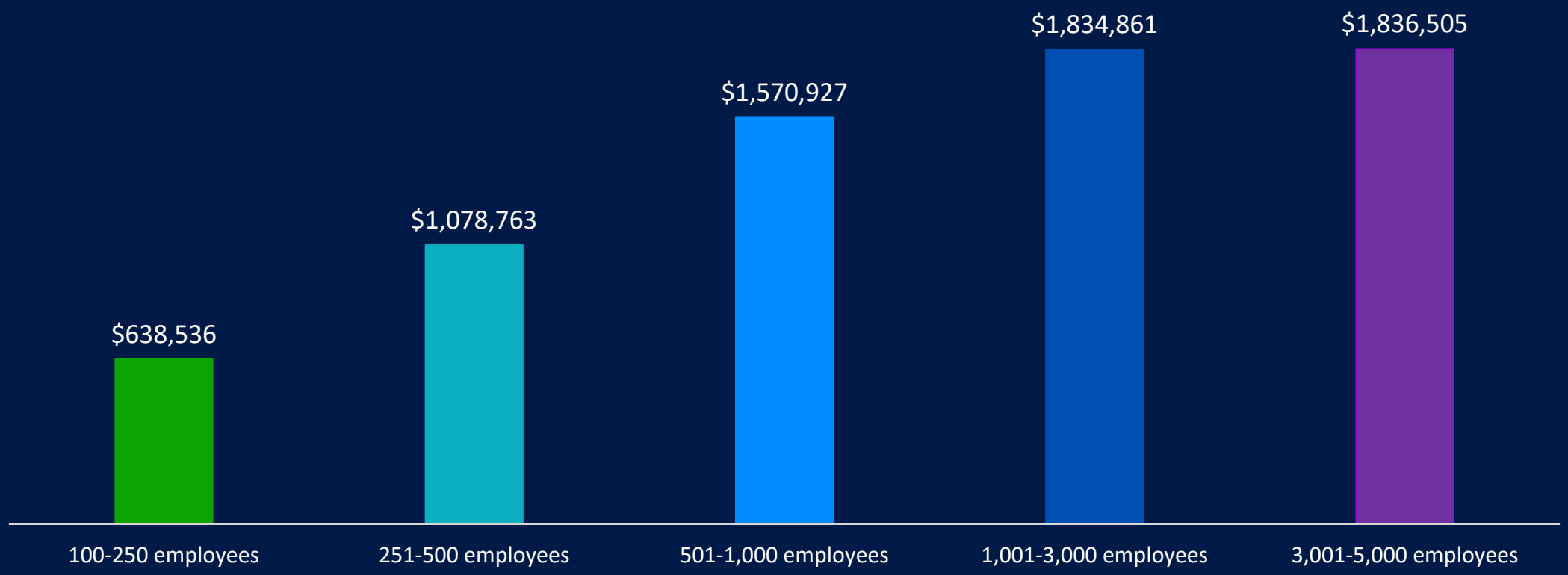
Did your organization get any data back? Yes, we paid the ransom and got data back; Yes, we used backups to restore the data. Base numbers in chart

SOPHOS

The Business Impact of Ransomware

Ransomware Recovery Cost | Organization Size

Mean recovery costs increase with organization size, before plateauing for organizations with 1,000 – 5,000 employees.



What was the approximate cost to your organization to rectify the impacts of the most significant ransomware attack (considering downtime, people time, device cost, network cost, lost opportunity etc.) excluding any ransom payments made?. n=3,400

SOPHOS

The Human Impact of Ransomware

Data Encryption | Impact on IT/Cybersecurity Team

41%	Increased **anxiety or stress** about future attacks
40%	Increased **pressure** from senior leaders
38%	Change of team **priorities/ focus**
38%	Ongoing increase in **workload**
37%	Changes to team/ organizational **structure**
34%	Feelings of **guilt** that the attack was not stopped
31%	Increased **recognition** from senior leaders
31%	Staff **absence** due to stress/ mental health issues
25%	Our team's leadership was **replaced**

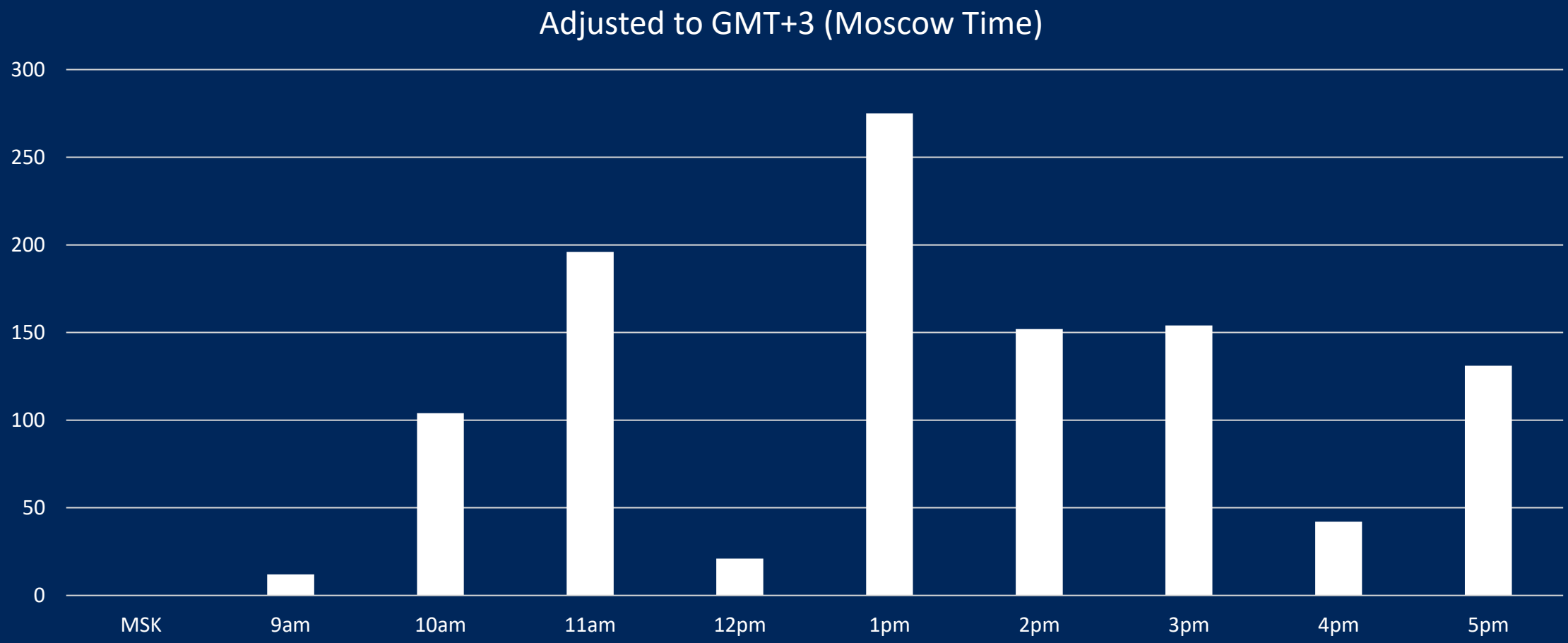
What repercussions has the ransomware attack had on the people in your IT/ cybersecurity team, if any?

SOPHOS

Who are behind these attacks?

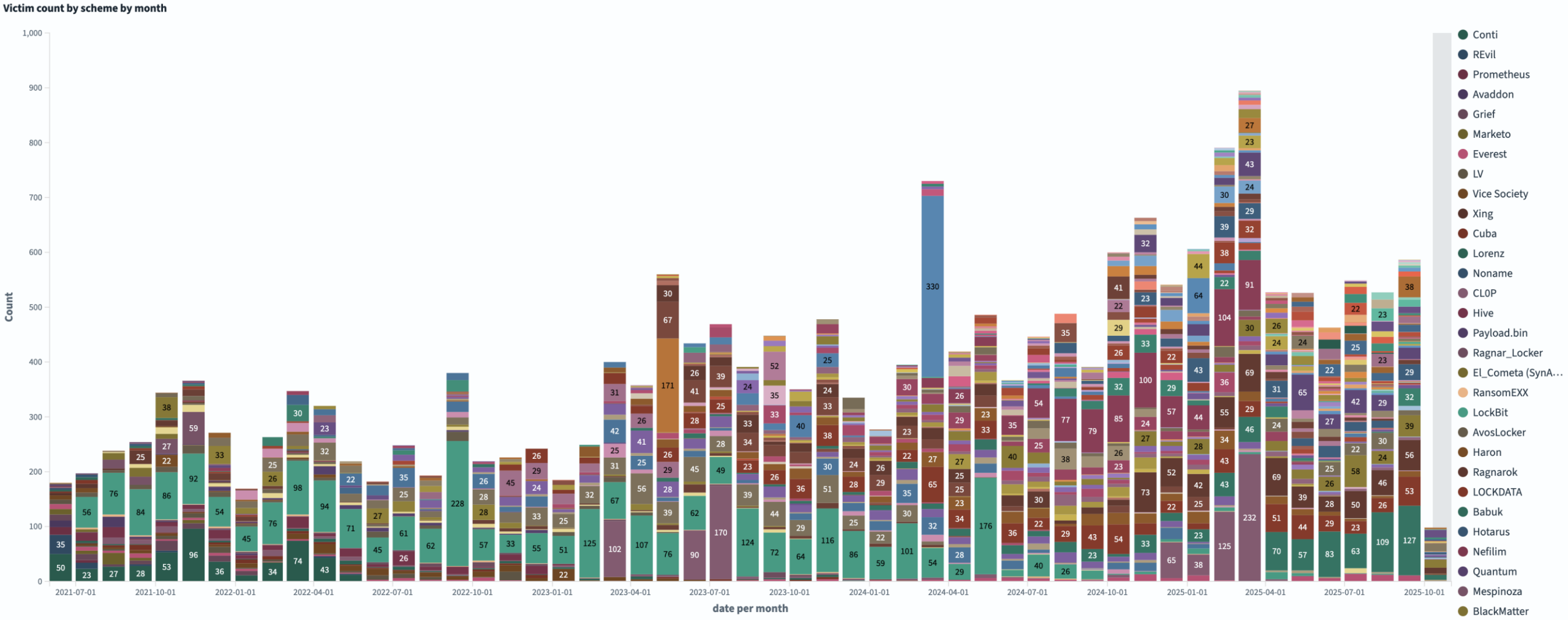
The Reality of Modern Cybercrime

Workin’ 9 to 5…..



SOPHOS

Key Protagonists



When The Bad Guys Disagree…..

CONTI NEWS

"WARNING"

The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

2/25/2022

"WARNING"

As a response to Western warmongering and American threats to use cyber warfare against the citizens of Russian Federation, the Conti Team is officially announcing that we will use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world. We do not ally with any government and we condemn the ongoing war. However, since the West is known to wage its wars primarily by targeting civilians, we will use our resources in order to strike back if the well being and safety of peaceful citizens will be at stake due to American cyber aggression.

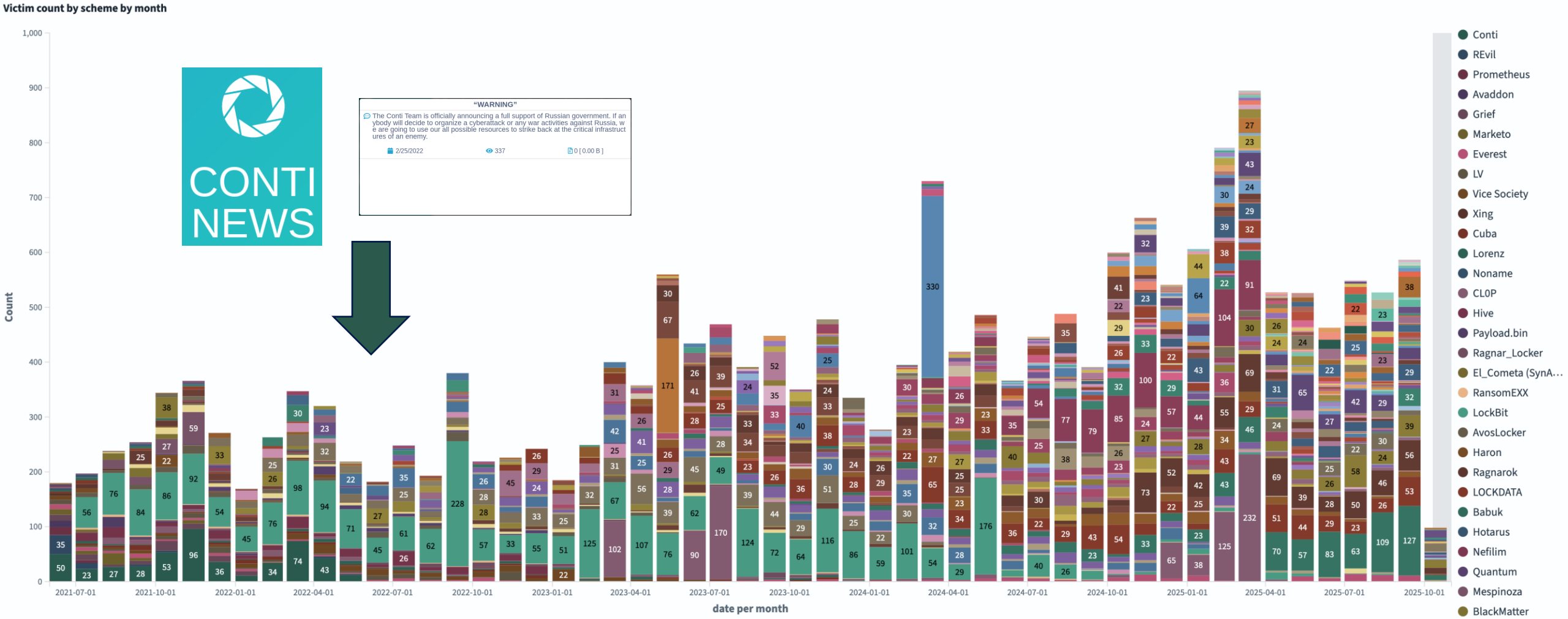
2/25/2022 477 0 [0.00 B]

TrickbotLeaks
@TrickbotLeaks

We have evidence of the FSB's cooperation with members of the Trickbot criminal group (Wizard Spiders, Maze, Conti, Diavol, Ruyk). Trickbot's deanonymization!

Joined March 2022

The Demise of Conti

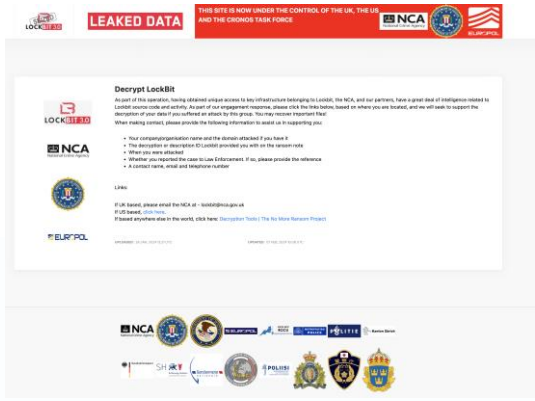


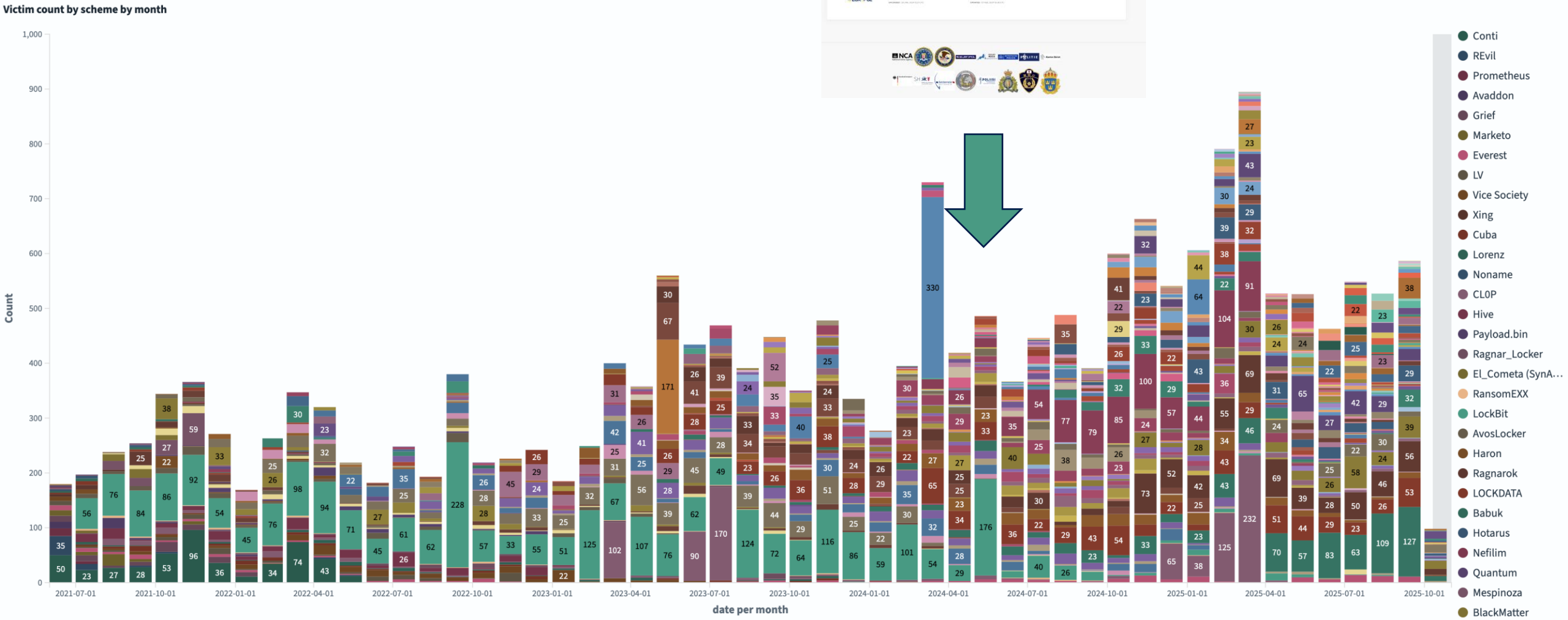
The Mythical Hydra

Key Protagonists


THE SITE
FORCEMENT
This site is now
with
in close cooperation
n Cronos'.
We can confirm th
disrupted as a resu
Enforcement actio
developing operati
Return here for mo
11:30 GMT on Tu
SEIZED
LOCKBIT 3.0
LEAKED DATA
THIS SITE IS NOW UNDER THE CONTROL OF THE UK, THE US AND THE CRONOS TASK FORCE
NCA National Crime Agency
EUROPOL
Press Releases
PUBLISHED
Updated: 01 Feb, 2024, 04:12 UTC 3947
LB Backend Leaks
PUBLISHED
NCA National Crime Agency
Updated: 31 Jan, 2024, 01:44 UTC 1182
Lockbitsupp
PUBLISHED
You've Been Banned From LOCKBIT 3.0
Updated: 31 Jan, 2024, 01:44 UTC 1182
Who is LockbitSupp?
2D 19H 30M 10S
The $10m question
Updated: 01 Feb, 2024, 04:12 UTC 3947
Lockbit Decryption Keys
PUBLISHED
LOCKBIT 3.0
Law Enforcement may be able to assist you to decrypt your Lockbit encrypted
Updated: 01 Feb, 2024, 04:12 UTC 3947
Recovery Tool
PUBLISHED
Japanese recovery tool key to access encrypted files and expand Europol's #Nomoreransom family
Updated: 01 Feb, 2024, 04:12 UTC 3947
US Indictments
PUBLISHED
FBI Investigation Leads to a Total of 5 LockBit Affiliates Charged By the Department of Justice. Two of Those Indictments Released Today.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Sanctions
0D 4H 0M 10S
United States Sanctions for Threat Actors Engaged in Significant Malicious Cyber Related Activity
Updated: 31 Jan, 2024, 01:44 UTC 1182
Arrest in Poland
PUBLISHED
On 20/02/2024 a suspected LockBit actor was arrested in Poland on the request of the French judicial authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Activity in Ukraine
PUBLISHED
On 20/02/2024 a suspected Lockbit actor was arrested in Ternopil (UA) by the local authorities.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Report Cyber Attacks!
PUBLISHED
Please report your Cyber Incident. To enable Law Enforcement to take protective and disruptive action, it is vital that victims report attacks and engage with Law Enforcement
Updated: 01 Feb, 2024, 04:12 UTC 3947
Cyber Choices
PUBLISHED
CYBER CHOICES
Updated: 01 Feb, 2024, 04:12 UTC 3947
StealBit down!
0D 19H 30M 10S
LOCKBIT 3.0
Learn more about LB's bespoke exfiltration tool, and how we have
Updated: 31 Jan, 2024, 01:44 UTC 1182
Affiliate infrastructure down
0D 19H 30M 10S
Law enforcement has compromised Lockbit platform and, as a result of this activity, other wide-ranging enabling, and affiliate (hacker), infrastructure, has been identified. This includes
Updated: 31 Jan, 2024, 01:44 UTC 1182
Lockbit's Hackers exposed
0D 19H 30M 10S
As a result of fully compromising Lockbit's platform, Law Enforcement will be coordinating activity to identify and deal with Lockbit's affiliates.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Prodaft
1D 19H 30M 10S
PRODAFT
Proactive Defense Against Future Threats
Updated: 31 Jan, 2024, 01:44 UTC 1182
Account Closures
1D 19H 30M 10S
In a targeted effort to undermine and combat the profit-generating ransomware machine, this operation paid particular attention to identifying and exploiting exfiltration channels.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Lockbit's new encryptor
1D 19H 30M 10S
TREND MICRO
Detailed analysis by Trend Micro on an in-development future iteration of Lockbit.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Secureworks
1D 19H 30M 10S
Secureworks
Lockbit in action; Three years of observations on affiliate tradecraft. Understand ransomware precursors and how to spot them.
Updated: 31 Jan, 2024, 01:44 UTC 1182
Lockbit Crypto
2D 19H 30M 10S
Over their 4 years in operation, we provide some insight into the profits they have made, and the financial impact of their
Updated: 31 Jan, 2024, 01:44 UTC 1182
Closure
4D 12H 29M 10S
This leak site (lockbit blog) to close.
NCA National Crime Agency
SOUTH WEST ROCU
METROPOLITAN POLICE
EUROPOL
POLITIE
Bundeskriminalamt
Kanton Zürich
Gendarmerie nationale
SH Schleswig-Holstein Landeskriminalamt
POLIISI KESKUSRIKOSPOLIISI
AUSTRALIAN FEDERAL POLICE

Operation CRONOS

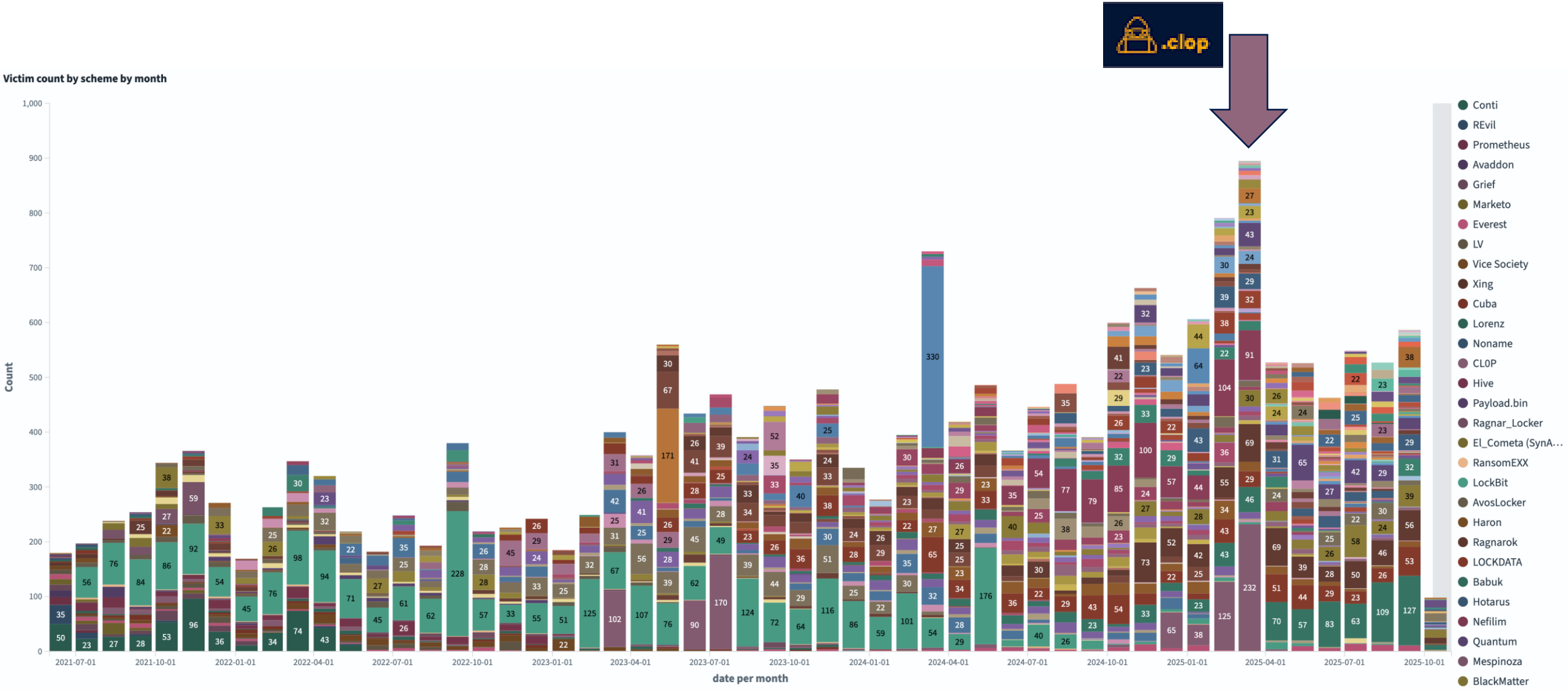


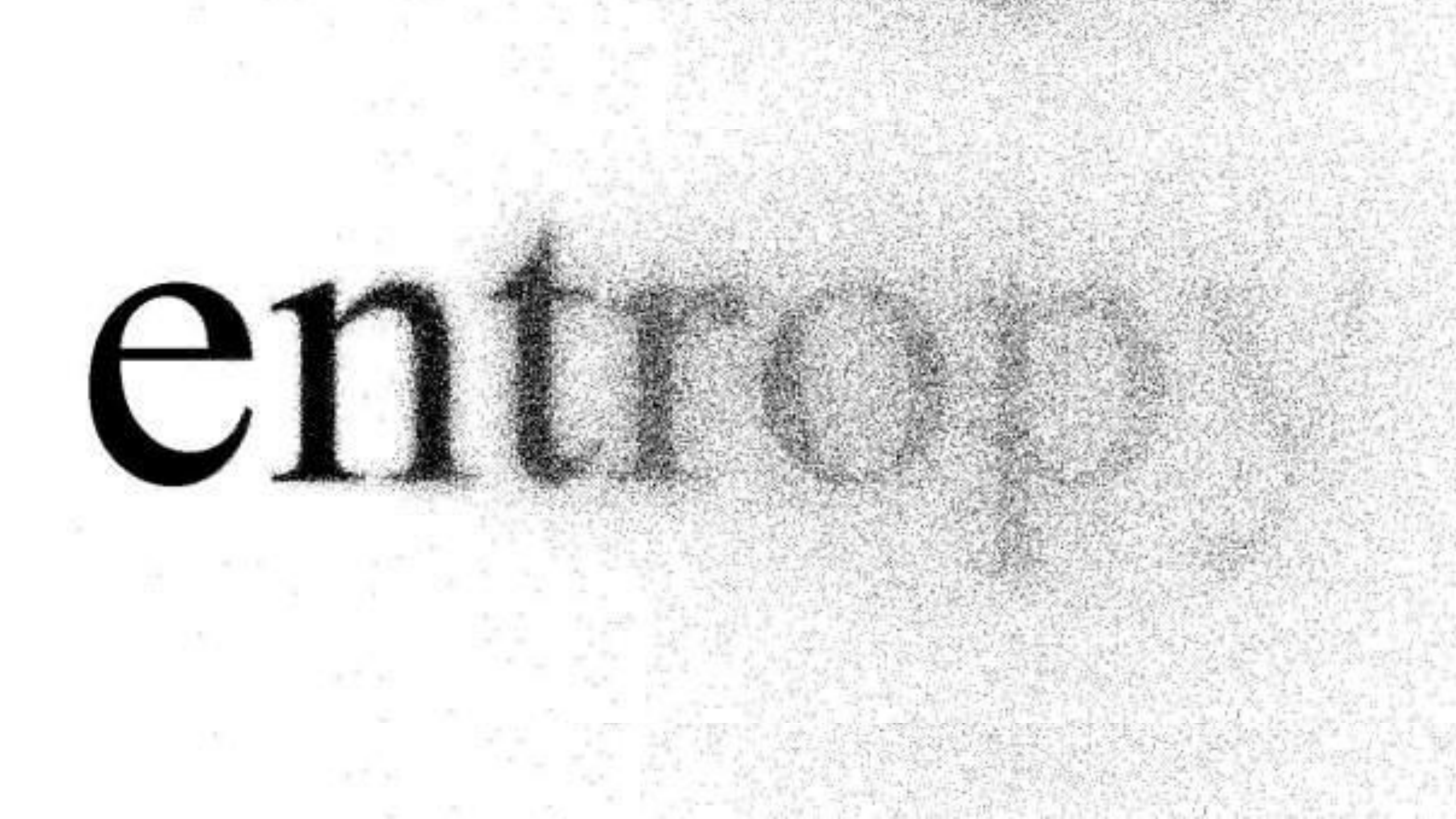


Functionally Untouchable

Gang Whack-A-Mole

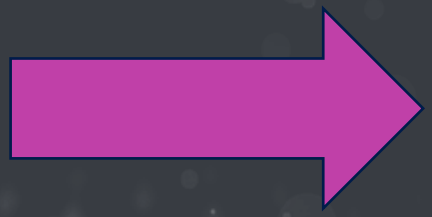
The Era of Quadruple Extortion



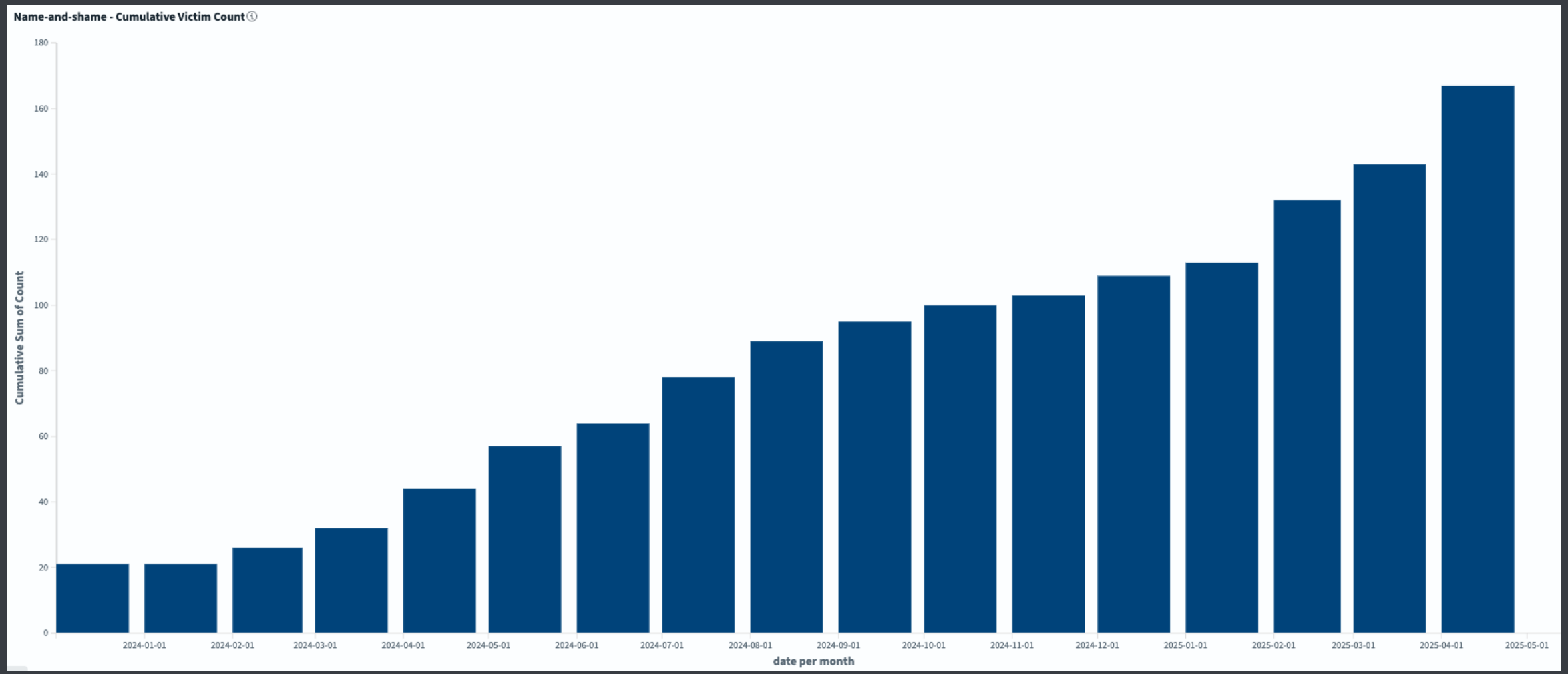

en


ثورة شعب
Dictator Leaves
Revolution

Enter the DragonForce

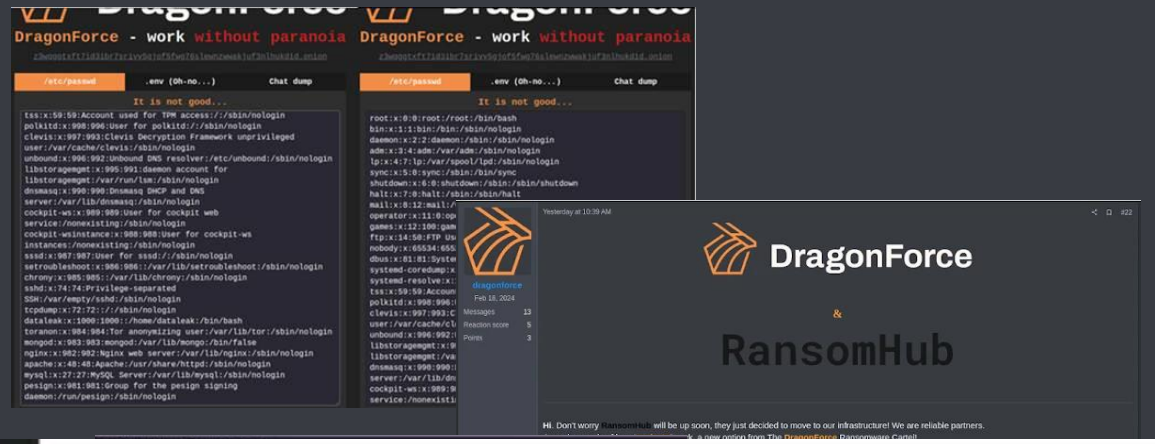


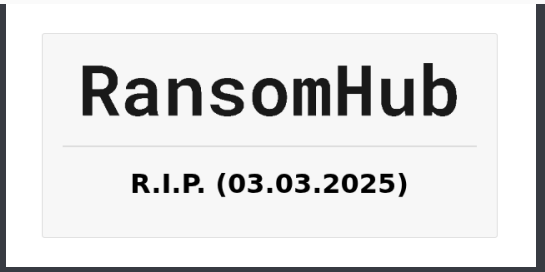
Victim Count



Aggressive Recruitment

- DragonForce have taken an aggressive approach to the recruitment of affiliates.
- Rival groups such as Mamona and BlackLock were all
- Dr
  wo
  Th
  op
- Ra
  de
  int
- Ra
  th
  fu





dragonforce
Feb 18, 2024
Messages 14
Reaction score 11
Points 3

DragonForce

The **DragonForce** Ransomware Cartel invites partners! The best tools, the best conditions and above all the reliability of the partner. We are the place where you will **receive stable payments** and **work without paranoia**.

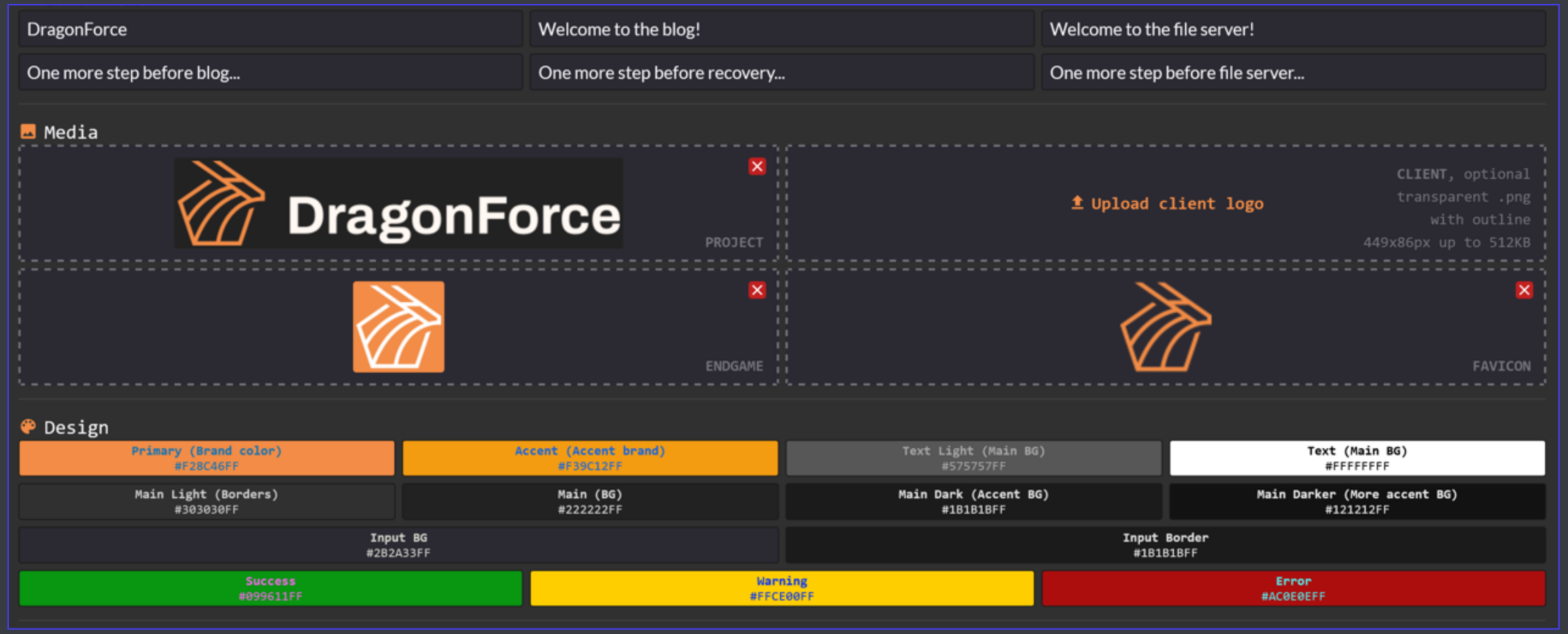
We offer you,

> • Complete automation of all work processes.
> • A complete system for managing your operations.
> • Combat software for every task! ESXi, NAS, BSD, Win.
> • Blog, FS (file server), admin panel, client panel.
> • DragonForce Anti-DDoS that works without interruption!
> • Reliable infrastructure!
> • Unlimited number of brands under one team!
> • The DragonForce Ransomware Cartel that monitors servers 24/7.
> • PETABYTEs, unlimited storage.
> • Free call-service, NTLM, Kerb decryption.
> • 80% goes to you (we only take 20%).

Windows works on all known versions of Windows, supports (full, header, partial) encryption modes.

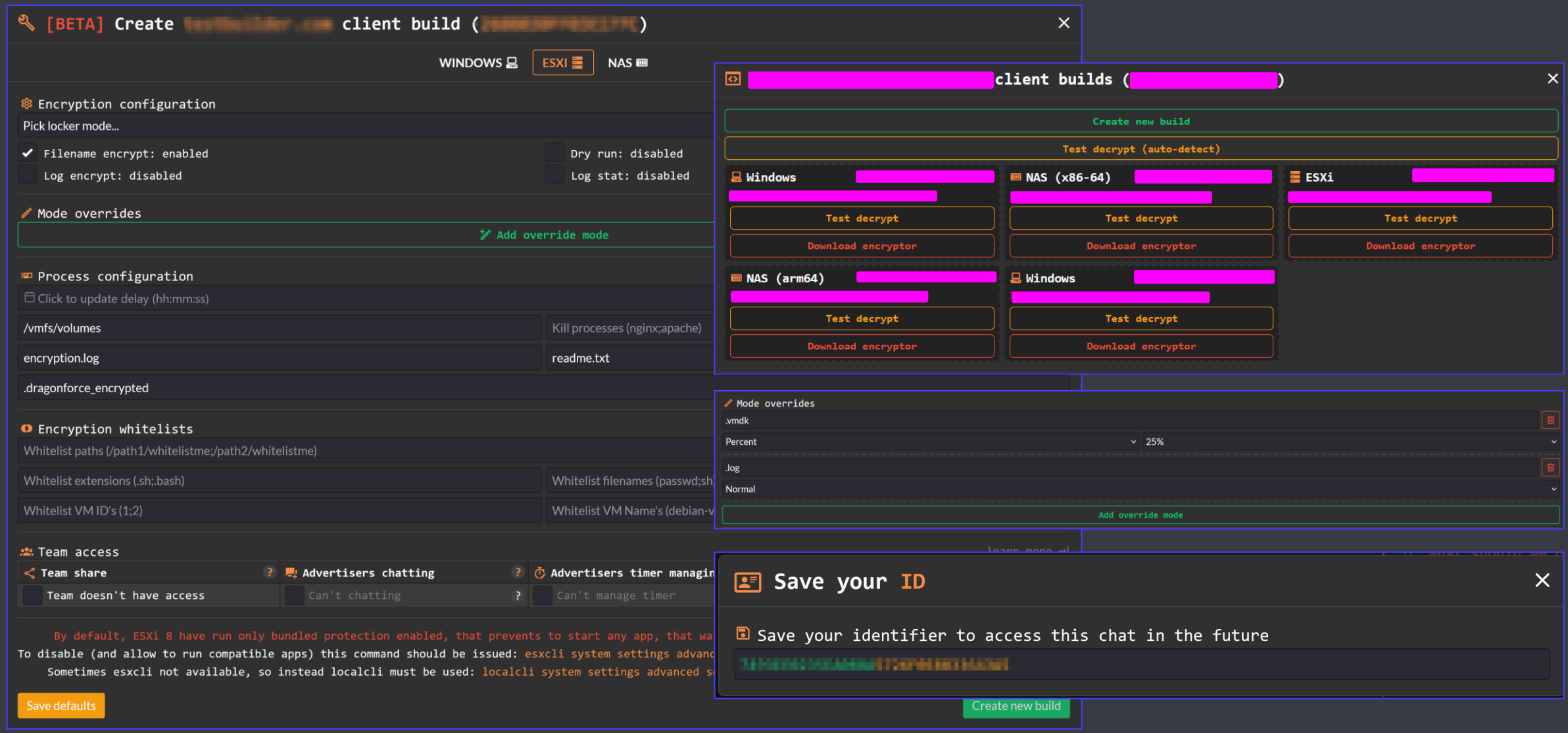
> • Mode overrides, you can customize encryption modes for individual files (full, header, partial).
> • Delayed start.
> • File name encryption, log encryption.
> • Work in local mode, network mode, or encrypt a single folder.

Customisable look and feel



SOPHOS

Configurable Options for their Ransomware Tools



SOPHOS

Hello!

Your files have been stolen from your network and encrypted with a strong algorithm. We work for money and are not associated with po

--- Our communication process:

1. You contact us.
2. We send you a list of files that were stolen.
3. We decrypt 1 file to confirm that our decryptor works.
4. We agree on the amount, which must be paid using BTC.
5. We delete your files, we give you a decryptor.
6. We give you a detailed report on how we compromised your company, and recommendations on how to avoid such situations in t

--- Client area (use this site to contact us):

Link for Tor Browser: http://3pktcrcbmssvrnwe5skburdwe2h3v6ibdnn5kbjqihsg6eu6s6b7ryqd.onion
>>> Use this ID: [redacted] to begin the recovery process.

* In order to access the site, you will need Tor Browser,
  you can download it from this link: https://www.torproject.org/

--- Additional contacts:

Support Tox: 1C054B722BCBF41A918EF3C485712742088F5C3E81B2FDD91ADEA6BA55F4A856D90A65E99D20

--- Recommendations:

DO NOT RESET OR SHUTDOWN - files may be damaged.
DO NOT RENAME OR MOVE the encrypted and readme files.
DO NOT DELETE readme files.

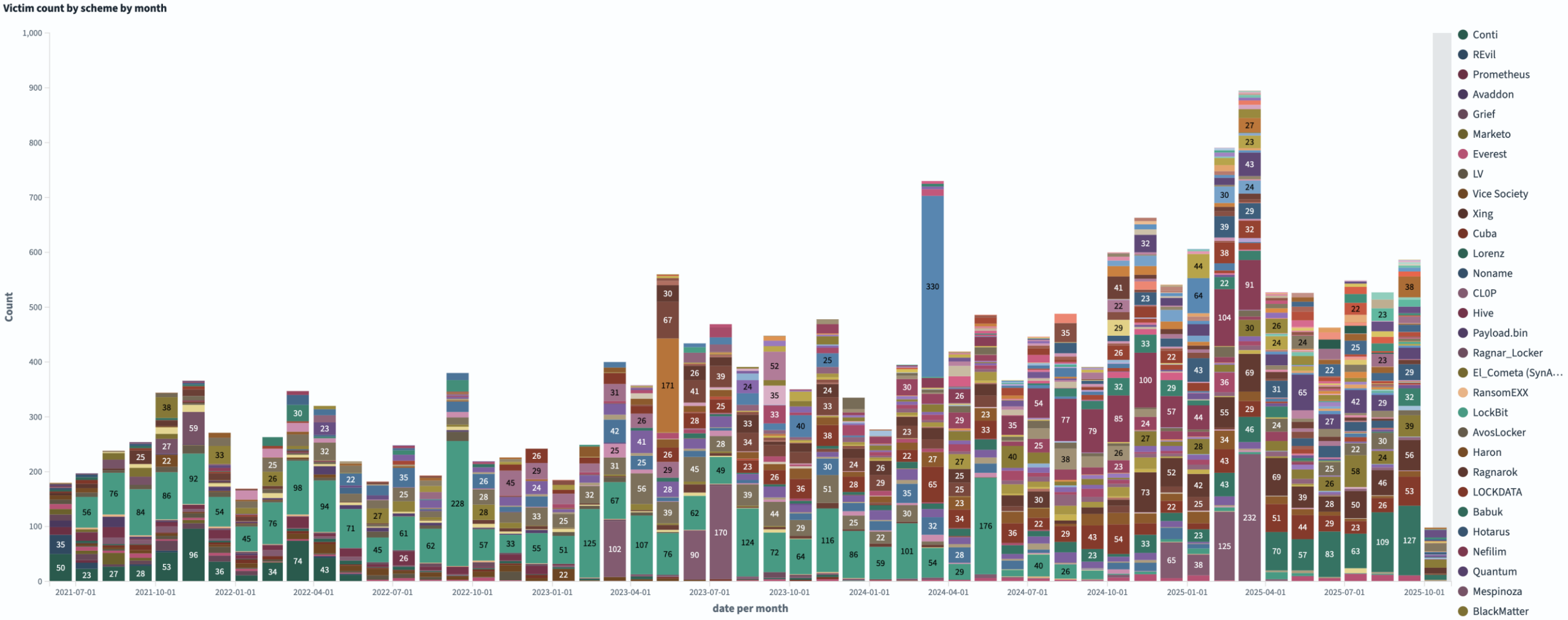
--- Important:

If you refuse to pay or do not get in touch with us, we start publishing your files.
06/04/2025 00:00 UTC the decryptor will be destroyed and the files will be published on our blog.

Blog: http://z3wqggtxft7id3ibr7srivv5gjof5fwg76slewnzwwakjuf3nlhukdid.onion

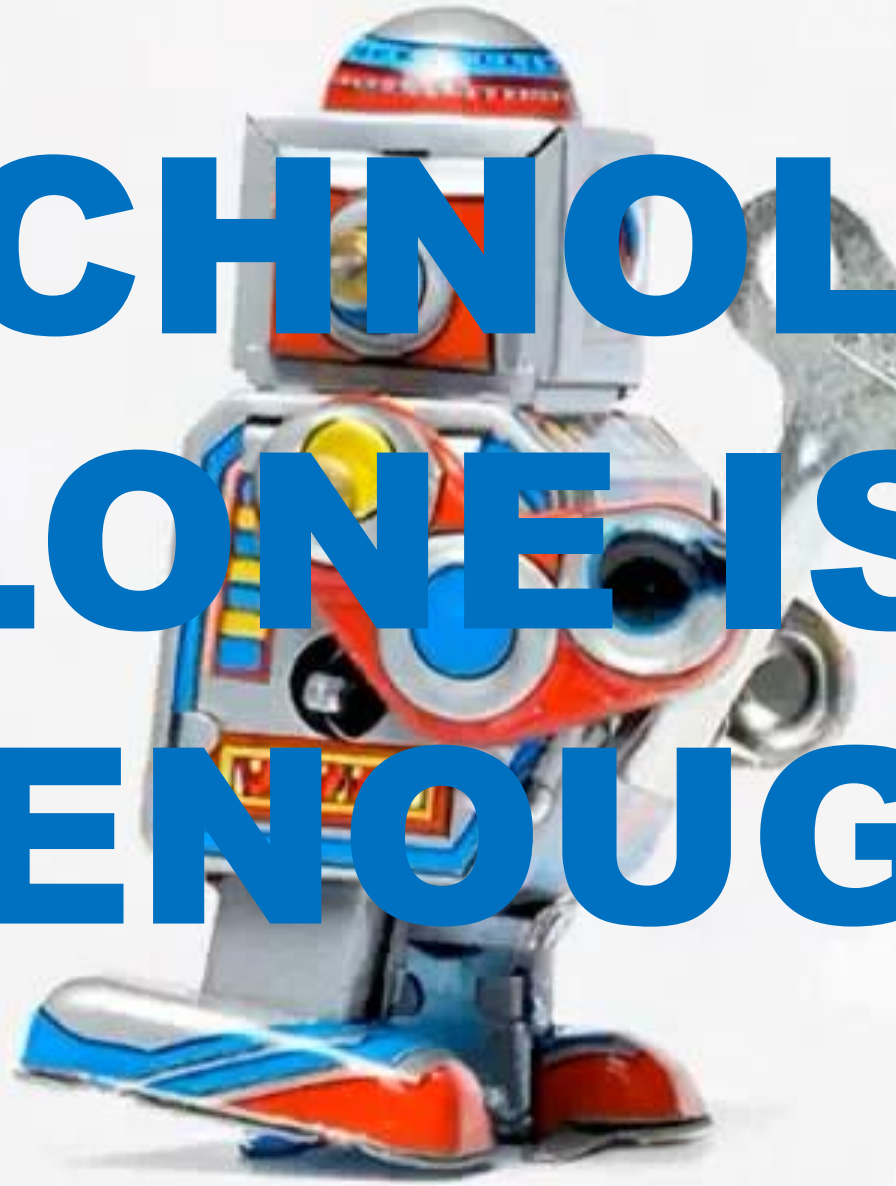
Sincerely, 01000100 01110010 01100001 01100111 01101111 01101110 01000110 01101111 01110010 01100011 01100101 [redacted]

Cartel Model of Ramsomware



Why Is This Important?

Human Resoruces



TECHNOLOGY ALONE ISN'T ENOUGH

How Active Adversaries Operate

MULTISTAGE ATTACKS

Attacks that end in a different place than they started

LIVING OFF THE LAND ATTACKS

Attacks that blend in by using legitimate tools in malicious ways

Exploiting Weakness

Attacks are timed to strike organisations at their weakest

CREDENTIAL ABUSE

Attacks that start with an adversary logging in instead of breaking in

So How Do I Combat These Challenges?

83%

Observable Advanced Warning Signs

The Challenge With Modern Day Threat Hunting


TECHNOLOGY
ALONE
ENOUGH
HUNTER.
TOOLS WON'T
MAKE YOU A

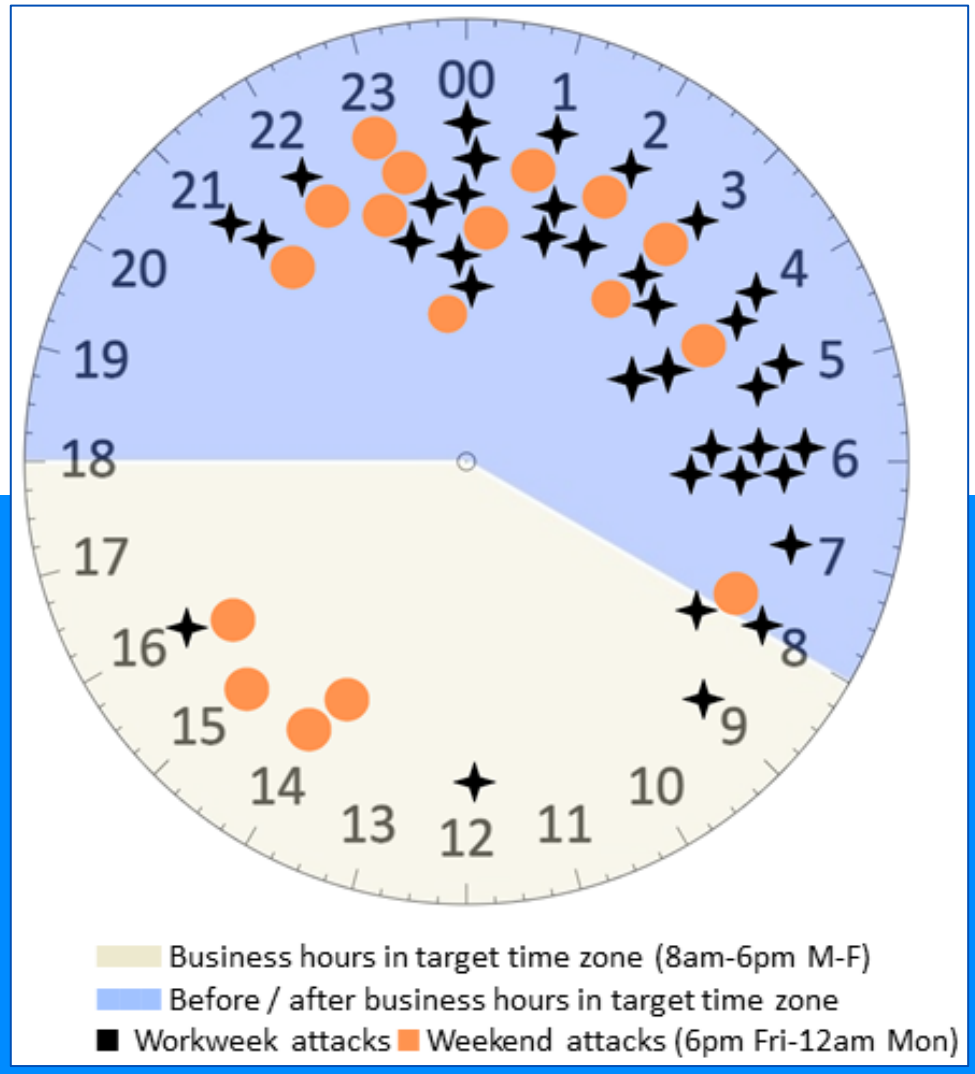

WORTH MORE THAN A GOOD
GLOVES AS
FIGHTER.

Cybersecurity has become too complex for most organizations to manage effectively.

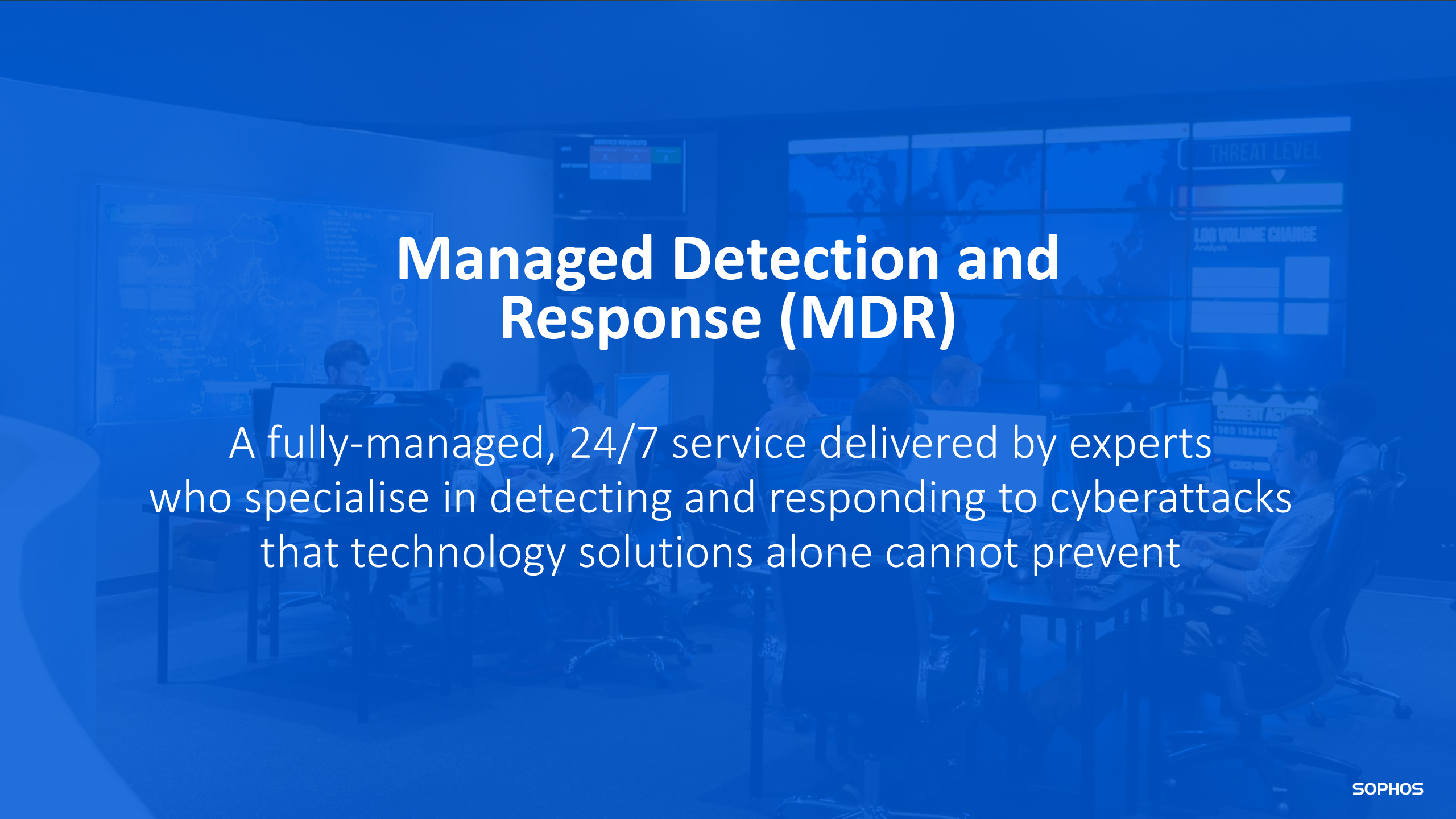
Attackers Target Off-Hours

91% of ransomware attacks start outside standard work hours

9 in 10 attacks occur outside 8am to 6pm on a weekday.



Source: Active Adversary Report for Tech Leaders, 2023, Sophos (n=52)



Managed Detection and Response (MDR)

A fully-managed, 24/7 service delivered by experts who specialise in detecting and responding to cyberattacks that technology solutions alone cannot prevent

SOPHOS

What Do The MDR Team Do?

MDR Service Philosophies

CROWDSTRIKE

SentinelOne

SOPHOS

SecurityHQ

ARCTIC WOLF

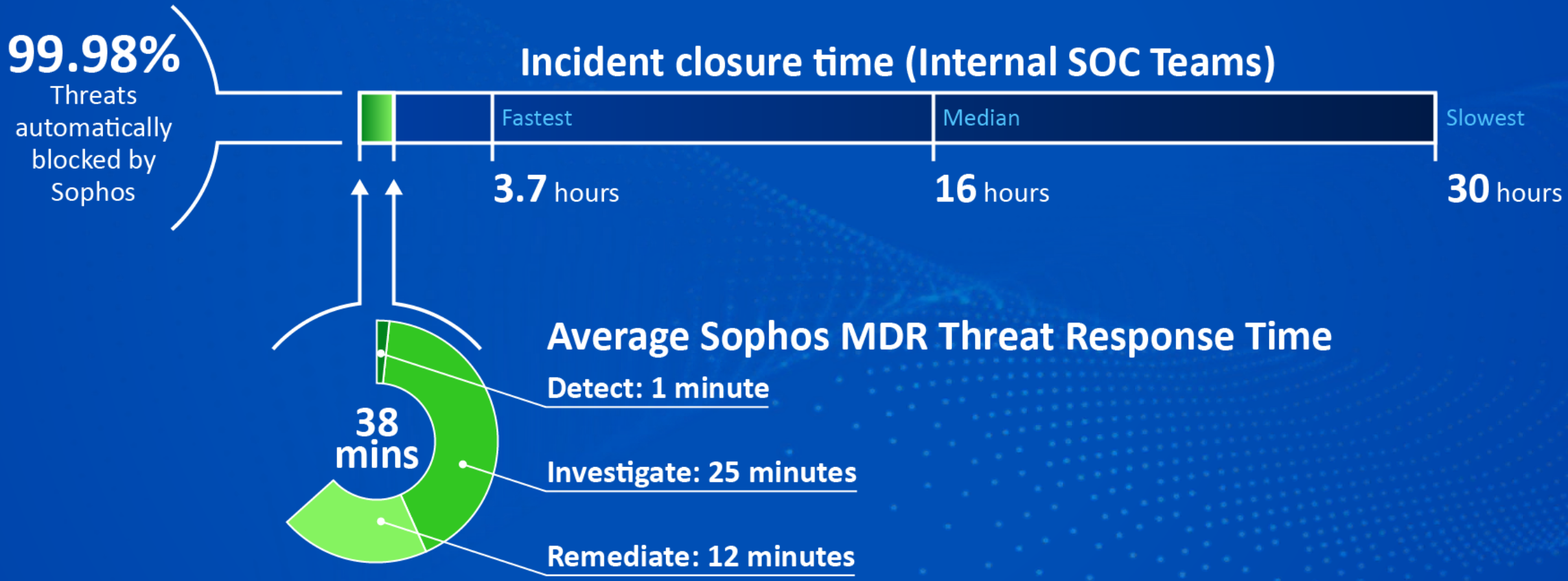
Vendor Tech + Service

Vendor Tech or BYO Tech + Service

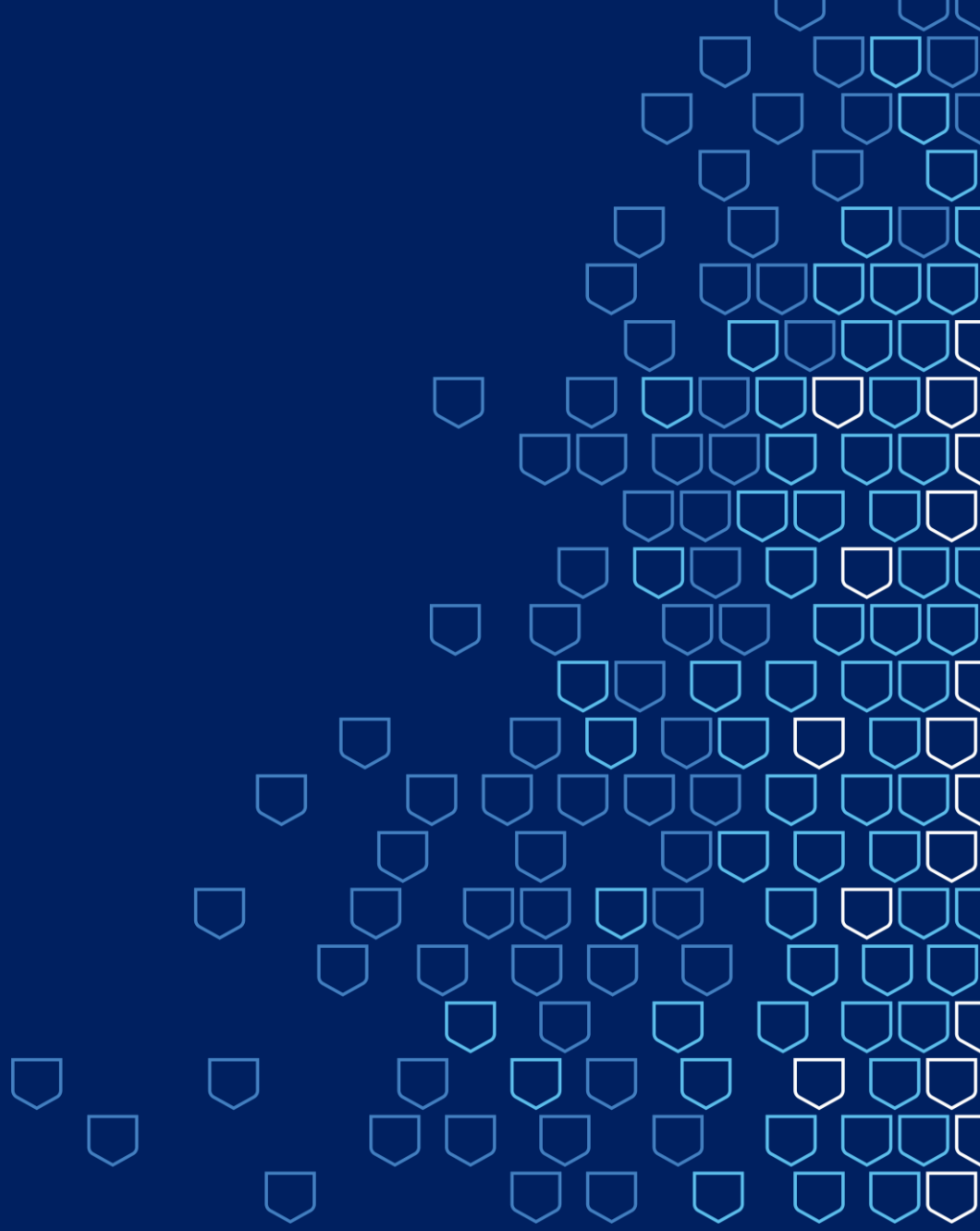
BYO Tech + Vendor Service

An Open Architecture Leads to Better Visibility

Investigation -> Remediation -> Resolution

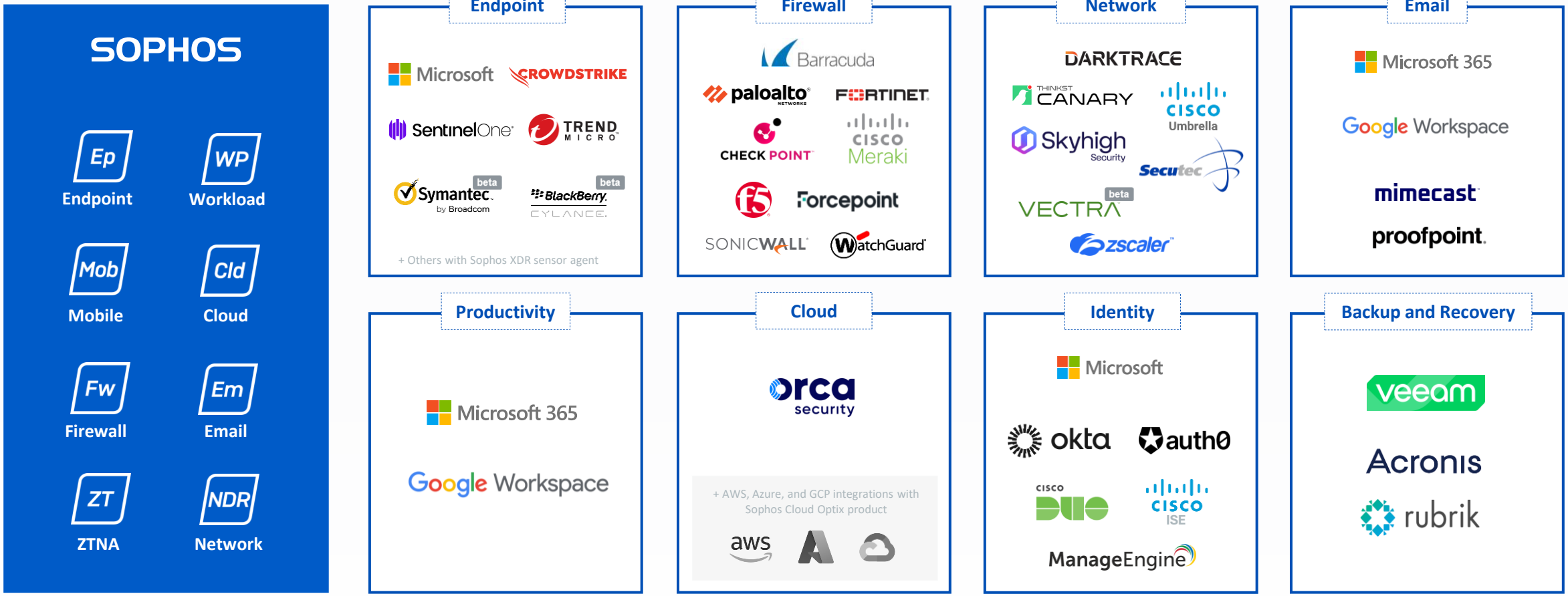


Delivering superior cybersecurity outcomes

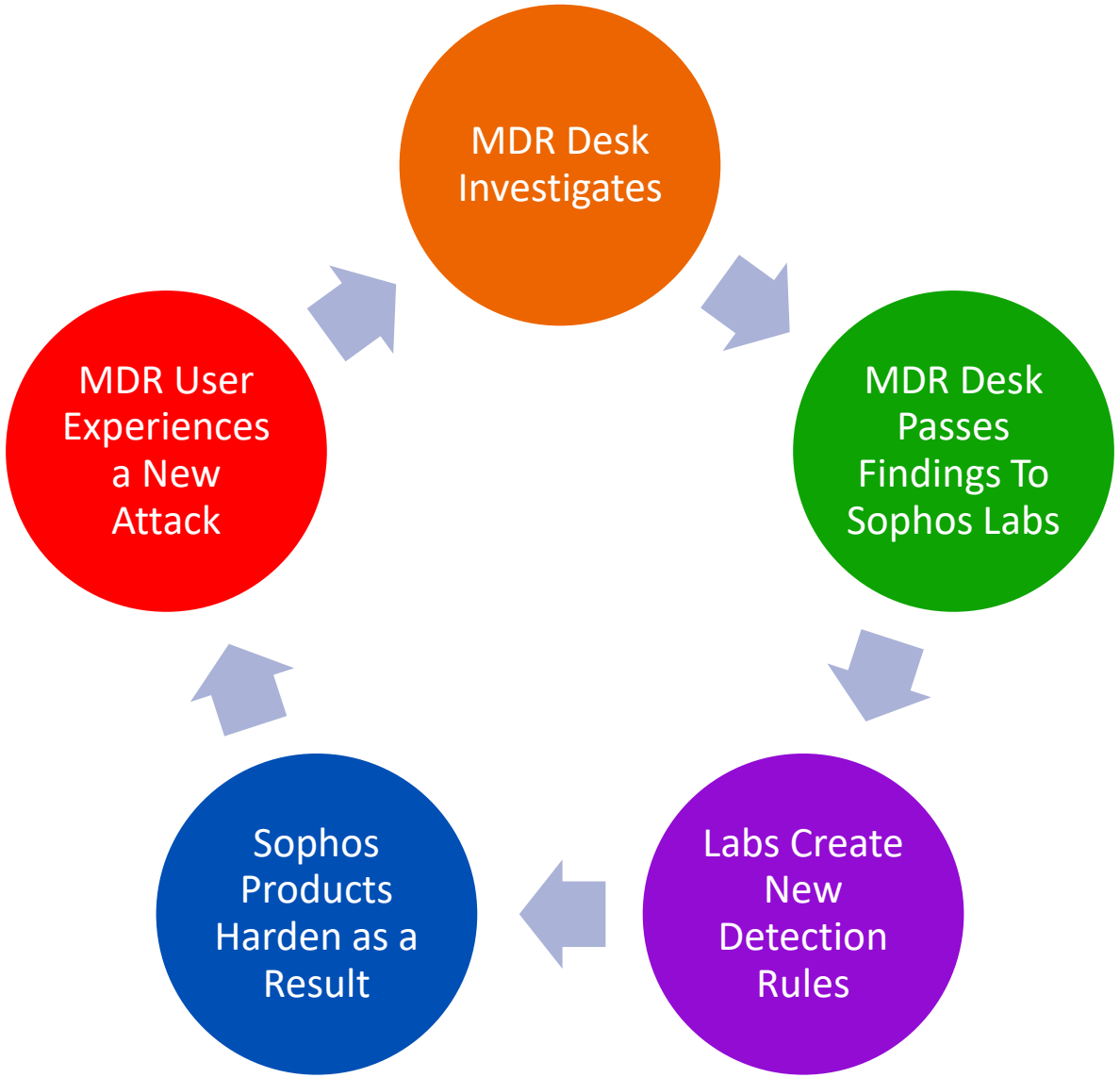


SOPHOS

More Integrations – Better Outcomes



A Virtuous Cycle



Wrap Up

Wrap Up

- Cybercrime is evolving
- Users are become a key focus of attacks and should be trained
- Technology alone is insufficient to protect against organized cybercrime
- Human-led attacks require human-led advanced threat hunting
- AI-empowered human threat hunters offer the best security outcomes